



DRIVENTO GROUP
GLOBAL DATA PROTECTION,
INFORMATION SECURITY AND
DATA GOVERNANCE POLICY

INTRODUCTION

Drivento LLC (“Drivento”, “the Company”) is a United States-based holding company operating as part of a broader corporate group that provides technology infrastructure, analytics, advisory services, operational platforms, and strategic solutions to insurance companies, reinsurance companies, brokers, and institutional participants within the global risk-transfer ecosystem.

The insurance and reinsurance industries depend heavily on the responsible handling of sensitive information including underwriting data, actuarial models, claims files, exposure information, financial records, and proprietary analytics. Because of the critical role that information plays in insurance markets, Drivento maintains a comprehensive enterprise data governance and cybersecurity framework designed to ensure the confidentiality, integrity, availability, and lawful use of information assets.

This Global Data Protection, Information Security, and Enterprise Data Governance Policy (“Policy”) establishes the governance framework through which Drivento manages, protects, processes, and secures data across its operations and across the entities that form part of the Drivento corporate group.

LEGAL NATURE AND ENFORCEABILITY

This Policy constitutes a binding and enforceable corporate governance instrument of DRIVENTO and may be incorporated by reference into, and form an integral and legally enforceable component of, any contractual relationship entered into by DRIVENTO or its affiliated entities.

This Policy is intended to have full legal effect in regulatory, contractual, and judicial proceedings across all applicable jurisdictions and shall be construed to the maximum extent permitted by law so as to ensure its validity, enforceability, and effectiveness against employees, contractors, and third parties with access to DRIVENTO systems or data.

CORPORATE STRUCTURE AND DATA ROLES

DRIVENTO LLC operates as the ultimate parent entity of the DRIVENTO corporate group. DRIVENTO SAS, a company duly incorporated and existing under the laws of the Republic of Colombia, and DRIVENTO S.A., a company duly incorporated and existing under the laws of the Republic of Guatemala, are wholly-owned subsidiaries of DRIVENTO LLC.

DRIVENTO SAS shall act as Data Controller with respect to personal data processed within the territory of the Republic of Colombia. DRIVENTO S.A., together with other affiliated entities within the DRIVENTO corporate group, may act as Data Processors or, where applicable, as Independent Data Controllers, strictly depending on the nature, scope, and purposes of the relevant processing activities.

The allocation of roles and responsibilities among such entities shall be determined in accordance with applicable law, intercompany agreements, and the functional involvement of each entity in the processing of personal data, and shall not be presumed solely by virtue of corporate affiliation.

All intra-group transfers are governed by binding corporate rules, internal agreements, and standardized data protection obligations.



APPLICABLE LAW AND JURISDICTION

This Policy shall be interpreted, enforced, and applied within a multi-jurisdictional legal framework, including the laws of the Republic of Colombia, the laws of the United States, and any applicable international data protection and privacy regulations.

To the fullest extent permitted by applicable law:

- (i) any matters arising within the territory of the Republic of Colombia, including the collection and processing of personal data by DRIVENTO SAS, shall be governed by and construed in accordance with the laws of Colombia;
- (ii) any matters relating to global infrastructure, cross-border data processing, or services performed by DRIVENTO LLC or its affiliated entities outside Colombia shall be governed by and construed in accordance with the laws of the State of Florida, United States, without regard to any conflict of law or choice of law principles that would result in the application of another jurisdiction's laws.

Any dispute, controversy, or claim arising out of or in connection with this Policy, including its interpretation, validity, or enforceability, shall be resolved in accordance with the dispute resolution and jurisdiction provisions set forth in the applicable contractual agreements, which shall prevail over this Policy in the event of any inconsistency or conflict.

In the absence of an applicable contractual provision, DRIVENTO reserves the right to determine the appropriate forum and jurisdiction, subject to applicable mandatory legal requirements.

DATA PROCESSING PRINCIPLES

All processing of personal data shall be conducted in strict compliance with applicable data protection laws and regulations and shall adhere to the principles of legality, necessity, proportionality, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability.

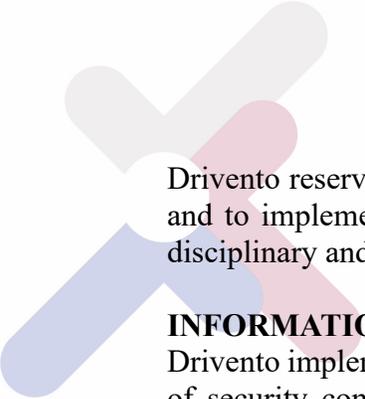
Personal data shall be processed solely for specified, explicit, and legitimate purposes, and only to the extent strictly necessary to fulfill such purposes. DRIVENTO shall implement appropriate technical and organizational measures to ensure and be able to demonstrate compliance with these principles at all times.

Any processing activity that does not meet these standards is strictly prohibited.

DATA GOVERNANCE AND CONTROL

Drivento maintains a centralized data governance framework with clearly defined and distributed operational accountability across its entities, business units, and functions.

Such framework is supported by enforceable audit rights, continuous monitoring mechanisms, and documented internal compliance controls designed to ensure adherence to applicable legal, regulatory, and corporate requirements.



Drivento reserves the right to audit, monitor, and verify compliance with this Policy at any time, and to implement corrective actions, including suspension of access, remediation measures, or disciplinary and contractual actions, in the event of non-compliance.

INFORMATION SECURITY

Drivento implements appropriate technical and organizational measures designed to ensure a level of security commensurate with the risks associated with the processing of personal data and sensitive information. Such measures include, without limitation, encryption, access controls, multi-factor authentication (MFA), logging, continuous monitoring, vulnerability management, and incident response capabilities, aligned with internationally recognized standards and best practices, including ISO 27001 principles and the NIST Cybersecurity Framework.

In furtherance of these objectives, Drivento may engage qualified third-party service providers to support the design, implementation, operation, and continuous improvement of its information security controls. All such third parties are subject to appropriate due diligence, contractual obligations, and confidentiality and data protection requirements.

The use of third-party service providers shall not be construed as a delegation of Drivento's core data protection obligations, except to the extent expressly permitted under applicable law and contractual arrangements.

THIRD-PARTY AND PLATFORM RISK ALLOCATION

All third parties engaged by Drivento are subject to written contractual arrangements that impose confidentiality, data protection, and information security obligations consistent with applicable law, regulatory requirements, and industry standards. Such arrangements may include data processing agreements, security requirements, and audit rights, as applicable.

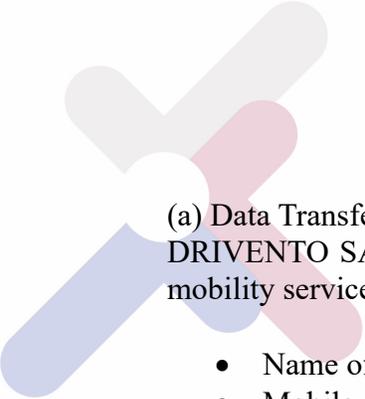
Drivento's responsibility is strictly limited to its own direct processing activities and to the obligations expressly assumed by it under applicable law and contractual arrangements. To the fullest extent permitted by applicable law, Drivento shall not be liable for any acts, omissions, failures, or independent processing activities of third parties, including those acting as independent data controllers or service providers.

No third party shall be deemed to act as an agent, representative, or extension of Drivento solely by virtue of a commercial or technical relationship, unless expressly agreed in writing. Any claims arising from the services or processing activities performed by such third parties shall be directed exclusively against the relevant third party.

The engagement of third parties in accordance with this Policy shall not be construed as a transfer or assumption of liability by Drivento beyond what is expressly required under applicable law.

SPECIAL CLAUSE – UBER AND THIRD-PARTY PLATFORMS (ENHANCED LIABILITY STRUCTURE)

When mobility services offered to the data subject are delivered through credits, vouchers, or technological integrations with platforms such as Uber Technologies Inc. or its affiliated entities ("Uber"), the following shall apply:



(a) Data Transfer and Purpose Limitation

DRIVENTO SAS may transmit certain personal data strictly necessary for the execution of the mobility service to Uber. Such data may include, without limitation:

- Name of the beneficiary;
- Mobile phone number;
- Service or voucher identifier;
- Operational information associated with the claim or granted benefit.

Such data transfer shall be carried out exclusively for the purpose of enabling and executing the mobility service requested by the data subject, in accordance with the purposes described in this Policy.

(b) Data Minimization

Only the minimum amount of personal data strictly necessary to enable the service shall be shared with Uber, in accordance with applicable data protection principles.

(c) Independent Controller Status

Uber shall act as an independent data controller with respect to any personal data processed through its platform. The processing of such data shall be governed by Uber's own privacy policies and terms, as made publicly available by Uber.

(d) No Control Over Third-Party Processing

DRIVENTO SAS does not control, influence, or determine the purposes or means of any subsequent processing carried out by Uber as an independent platform operator.

(e) User Acknowledgment and Acceptance

By using or accepting the mobility service, the user expressly acknowledges and agrees that:

DRIVENTO acts solely as a technological intermediary facilitating access to third-party mobility services;

Uber operates independently and is solely responsible for the provision of transportation services and any associated data processing;

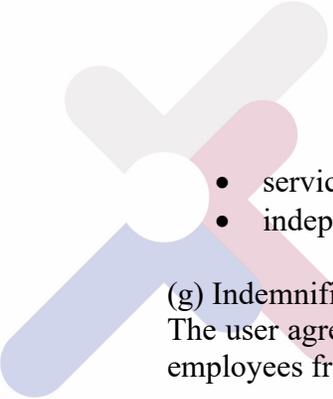
Uber's services are subject exclusively to Uber's own terms, conditions, and privacy policies;

Any claim, complaint, or dispute related to Uber's services must be directed exclusively against Uber.

(f) Waiver of Claims

To the maximum extent permitted by applicable law, the user expressly waives any and all claims against DRIVENTO arising from or related to:

- acts or omissions of Uber;

- 
- service failures, delays, or disruptions attributable to Uber;
 - independent data processing carried out by Uber.

(g) Indemnification

The user agrees to indemnify, defend, and hold harmless DRIVENTO, its affiliates, officers, and employees from and against any claims, damages, liabilities, or expenses arising from:

- misuse of the mobility service;
- breach of applicable terms governing third-party platforms;
- any act or omission attributable to the user in connection with such services.

(h) Limitation of Liability

To the fullest extent permitted by applicable law, DRIVENTO shall not be liable for any indirect, incidental, consequential, special, or punitive damages, including but not limited to loss of data, business interruption, or loss of opportunity, arising from or related to the use of third-party mobility platforms.

(i) Risk Allocation and Nature of Service

The user expressly understands and agrees that DRIVENTO is not a transportation provider and does not own, operate, or control any vehicles or drivers. DRIVENTO's role is strictly limited to facilitating access to third-party mobility services through technological means.

CROSS-BORDER DATA TRANSFERS

Any transfer of personal data, including cross-border transfers, shall be subject to appropriate safeguards designed to ensure an adequate level of protection consistent with applicable data protection laws and regulations.

Such safeguards may include, without limitation, contractual mechanisms (including standard contractual clauses or equivalent instruments), internal compliance frameworks, and appropriate technical and organizational security measures.

Where required by applicable law, DRIVENTO shall assess the legal and regulatory environment of the recipient jurisdiction and implement supplementary measures as necessary to ensure that the transferred data is afforded a level of protection essentially equivalent to that provided under applicable law.

All transfers shall be conducted in a manner that ensures the integrity, confidentiality, and security of personal data throughout the transfer process.

DATA SUBJECT RIGHTS

Data subjects shall retain the rights afforded to them under applicable data protection laws and regulations, including, where applicable, the rights of access, rectification, erasure, restriction of processing, objection, and data portability.

The exercise of such rights shall be subject to appropriate identity verification procedures and may be limited where necessary to comply with applicable legal, regulatory, contractual, or operational

obligations, including obligations relating to data retention, fraud prevention, dispute resolution, and the establishment, exercise, or defense of legal claims.

DRIVENTO reserves the right to deny or limit any request to the extent permitted by applicable law, including where such request is manifestly unfounded, excessive, or would adversely affect the rights and freedoms of third parties.

INCIDENT RESPONSE AND BREACH NOTIFICATION

Drivento maintains a formal incident response and data breach management program designed to detect, assess, contain, investigate, and remediate security incidents, including those involving personal data or confidential information.

Such program is aligned with applicable legal and regulatory requirements and incorporates procedures for risk assessment, internal escalation, documentation, and remediation.

Where required by applicable law, Drivento shall notify competent supervisory authorities and, where applicable, affected data subjects within the timeframes and in the manner prescribed by law.

Drivento reserves the right to determine the appropriate scope, timing, and content of any notification to the extent permitted by applicable law and based on a reasonable assessment of the risks associated with the incident.

LIMITATION OF LIABILITY (GLOBAL)

To the fullest extent permitted by applicable law, Drivento shall not be liable for any indirect, incidental, consequential, special, exemplary, or punitive damages, whether foreseeable or unforeseeable, arising out of or in connection with this Policy, the use of its services, or the processing of data.

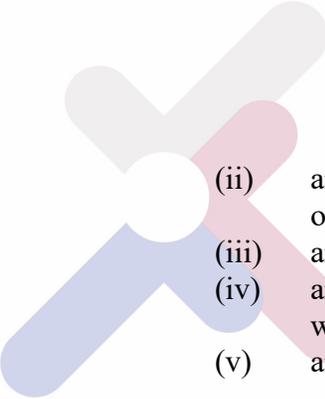
This limitation includes, without limitation, damages for loss of data, loss of profits, loss of revenue, loss of business opportunities, business interruption, reputational harm, or any other economic or intangible losses, even if Drivento has been advised of the possibility of such damages.

The foregoing limitation shall apply regardless of the form of action, whether in contract, tort (including negligence), strict liability, or otherwise, and shall extend to any claims arising from the acts or omissions of third-party service providers, to the extent permitted by applicable law.

INDEMNIFICATION

To the fullest extent permitted by applicable law, users, clients, and partners agree to indemnify, defend, and hold harmless Drivento, its parent company, subsidiaries, affiliates, officers, directors, employees, agents, and representatives from and against any and all claims, demands, actions, damages, losses, liabilities, costs, and expenses (including, without limitation, reasonable attorneys' fees and legal costs) arising out of or in connection with:

- (i) any misuse or unauthorized use of the services;

- 
- (ii) any breach of this Policy, applicable terms and conditions, or any legal or regulatory obligation;
 - (iii) any act or omission by the user, client, or partner in connection with the services;
 - (iv) any interaction with, or use of, third-party platforms or service providers (including, without limitation, mobility platforms such as Uber); or
 - (v) any violation of the rights of any third party, including privacy or data protection rights.

Drivento reserves the right, at its own discretion, to assume the exclusive defense and control of any matter subject to indemnification, in which case the indemnifying party shall cooperate fully with Drivento in asserting any available defenses. The indemnifying party shall not settle any claim without Drivento's prior written consent, which shall not be unreasonably withheld.

AUDIT AND ENFORCEMENT

Drivento reserves the right, at any time and with or without prior notice (to the extent permitted by applicable law), to audit, monitor, and verify compliance with this Policy, including through the review of systems, processes, records, and relevant documentation, whether maintained internally or by third parties acting on its behalf.

In the event of actual or suspected non-compliance, Drivento may, in its sole discretion, implement any corrective or protective measures deemed appropriate, including, without limitation:

- (i) suspension or termination of system access;
- (ii) restriction of data processing activities;
- (iii) mandatory remediation actions;
- (iv) enforcement of contractual rights and remedies; and
- (v) initiation of disciplinary, administrative, or legal proceedings.

The exercise of such rights shall be without prejudice to any other rights or remedies available to Drivento under applicable law or contract.

POLICY UPDATES

Drivento reserves the right, at its sole discretion, to update, modify, or replace this Policy at any time to reflect regulatory developments, operational changes, technological advancements, or risk management considerations.

Any updated version of this Policy shall become effective upon its publication or communication through Drivento's official channels, unless a later effective date is required by applicable law.

Continued use of Drivento's services or systems following such update shall constitute acceptance of the revised Policy, to the extent permitted by applicable law.

Drivento shall not be required to provide individualized notice of such updates, except where mandated by applicable law.

EFFECTIVE DATE

This Policy is effective upon publication and supersedes prior versions.